De verplichting tot het bijwerken van onveilige software na Consumentenbond/Samsung

De invloed van informatie- en communicatietechnologie op ons dagelijkse leven blijft toenemen. Dit komt mede doordat steeds meer apparaten, al dan niet onder de noemer van het 'internet of things', voorzien zijn van software en toegang tot het internet. Deze ontwikkeling brengt naast voordelen ook risico's met zich. De microfoon in een 'smart speaker' kan bijvoorbeeld worden afgeluisterd door criminelen en (buitenlandse) veiligheidsdiensten. Dergelijke apparaten met '*embedded*' software kunnen daarnaast deel gaan uitmaken van een 'botnet' en worden gebruikt voor DDoS-aanvallen.

De beveiliging ('cybersecurity') van deze soft- en hardware staat daarom hoog op de nationale en Europese agenda. Deze aandacht strekt zich ook uit tot de juridische dimensie van dit onderwerp. Zo creëert het voorstel voor de 'Cybersecurity Act' een juridische basis voor de ontwikkeling van Europese standaarden en certificaten.[1] Het Nederlandse kabinet pleit daarnaast voor de formulering van minimumeisen, bijvoorbeeld in het kader van de voorgestelde richtlijn digitale inhoud, de evaluatie van de productaansprakelijkheidsrichtlijn en de radioapparatuurrichtlijn.[2]

Tegelijkertijd bestaat het besef dat een juridische verplichting om software te beveiligen ook kan worden gebaseerd op de bestaande open normen in het Burgerlijk Wetboek.[3] De precieze omvang van deze cybersecurityplicht blijkt echter niet uit de rechtspraak. Zonder deze duidelijkheid is het voor individuele consumenten niet aantrekkelijk om een procedure te starten.[4]

Een collectieve actie in de zin van art. 3:305a BW kan deze patstelling doorbreken. In het conflict dat heeft geleid tot Rb. Den Haag 30 mei 2018, ECLI:NL:RBDHA:2018:6310 (*Consumentenbond/Samsung*) eist de Consumentenbond (kortgezegd) dat Samsung de beveiliging van zijn telefoons ten minste vier jaar na de introductie en twee jaar na de verkoop blijft bijwerken. Hij eist in het bijzonder dat Samsung kwetsbaarheden repareert die Google als 'kritiek' heeft aangemerkt en waarvoor een update beschikbaar is. De Consumentenbond eist daarnaast software*upgrades* en betere informatie over het updatebeleid. Deze vorderingen zijn eerder in een kort geding afgewezen op grond van het ontbreken van spoedeisend belang.[5]

In de bodemprocedure oordeelt de rechter dat niet "ter discussie staat dat in dit verband van Samsung kan worden verwacht dat zij voldoende adequaat en doeltreffend optreedt tegen de hiervoor omschreven veiligheidsrisico's van door Google als critical aangemerkte kwetsbaarheden". Toch wijst de rechtbank de vordering tot het bijwerken van de beveiliging om verschillende redenen af. De Consumentenbond beraadt zich nog op vervolgstappen.

De rechtbank oordeelt dat de Consumentenbond niet-ontvankelijk is voor zover de vordering betrekking heeft op de toekomst. Zij stelt dat de onrechtmatigheid van het handelen van Samsung niet kan worden losgezien van de toekomstige (technische) omstandigheden van het geval. Het niet-bijwerken van de software is daarom niet in alle mogelijke toekomstige gevallen onrechtmatig. Het is bovendien niet zeker dat iedere door Google als 'kritiek' aangemerkte kwetsbaarheid tot reële risico's leidt die door een update moeten worden weggenomen.

De rechtbank oordeelt verder dat Samsung voldoende doet om de kwetsbaarheden te verhelpen. Zij overweegt hiervoor onder andere dat het verstrekken van updates een complex proces is waarbij verschillende partijen zijn betrokken, dat Samsung bij het updaten van de vele verschillende modellen prioriteiten mag aanbrengen op basis van het concrete dreigingsniveau en technische en economische afwegingen en dat nieuwere versies niet altijd goed werken op oudere telefoons.

Deze complicaties illustreren dat het bijwerken van software een complex proces kan zijn. Zij doen echter geen afbreuk aan de verplichting van Samsung. Zelfs als het bedrijf de verstrek-

1. European Commission, *Proposal for a Regulation on the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")*, COM(2017) 477 final, 2017.
2. *Nederlandse Cybersecurity Agenda. Nederland digitaal veilig*, 2018, p. 27-29; Ministerie van Economische Zaken en Klimaat & Ministerie van Justitie en Veiligheid, *Roadmap. Digitaal Veilige Hard- en Software*, 2018, p. 24-26; M.C.G. Keijzer, *Beantwoording vragen over onveilige telefoons van Samsung* (Brief aan de Tweede Kamer van 28 juni 2018).
3. Zie onder andere noot 2; P.T.J. Wolters & C.J.H. Jansen, *Ieder bedrijf heeft digitale zorgplichten*, Den Haag: Cyber Security Raad 2017; H. Gelevert, A. Smulders & P. van den Brink, *Digitaal Veilige Hard- en Software*, Den Haag: TNO 2017, p. 65.
4. P.W.J. Verbruggen & P.T.J. Wolters, 'Consument en cybersecurity. Een agenda voor Europese Harmonisatie van zorgplichten', *TvCh* 2017, afl. 1, p. 22.
5. Rb. Amsterdam (vzr.) 8 maart 2016, ECLI:NL:RBAMS:2016:1175. Zie hierover P.T.J. Wolters & P.W.J. Verbruggen, 'De verplichting tot het bijwerken van onveilige software', *WPNR* 2016, afl. 7123, p. 832-839.

king van updates niet volledig in eigen hand heeft, is het ten minste verplicht om zijn deel van het proces op tijd af te ronden. De vordering van de Consumentenbond houdt hier, met betrekking tot de rol van Google, ook rekening mee. Samsung kiest er bovendien zelf voor om een grote hoeveelheid verschillende modellen aan te bieden. De omstandigheid dat *upgrades* met nieuwe functionaliteiten niet altijd op oude telefoons werken, betekent ten slotte niet dat het ook niet mogelijk is om de beveiliging van deze telefoons bij te werken.

Hoewel de overwegingen van de rechtbank niet allemaal overtuigend zijn, illustreren zij de obstakels waar een belangenorganisatie tegen aan kan lopen. De vordering van de Consumentenbond is niet alleen gericht tegen Samsung, maar heeft tevens het doel om ook andere ontwikkelaars van (embedded) software tot regelmatige updates te bewegen.[6] De Rechtbank Den Haag legt echter de nadruk op de complexe, steeds veranderende omstandigheden van het concrete geval. Zij wijst de algemeen geformuleerde vordering daarom af.

Hierdoor rijst de vraag of een concretere vordering wel voor toewijzing in aanmerking komt. Een belangenorganisatie zou bijvoorbeeld een verklaring voor recht kunnen vorderen dat het niet-bijwerken van de beveiliging gedurende een bepaalde periode op grond van een tijdens die periode bestaande kwetsbaarheid onrechtmatig is. De uitspraak van de rechtbank laat echter zien dat ook deze vordering niet altijd toewijsbaar zal zijn.

De Consumentenbond onderbouwt zijn vorderingen door te wijzen op verschillende kwetsbaarheden, waaronder 'Stagefright' en 'Stagefright 2.0'. De rechtbank overweegt dat deze beveiligingslekken ondertussen verholpen zijn. De Consumentenbond heeft hierdoor geen belang meer bij een gebod om deze kwetsbaarheden te verhelpen.[7] Zijn belang bestaat hoogstens uit de proceskosten. Samsung kan bovendien ook dit belang wegnemen door deze kosten te vergoeden of de beveiliging bij te werken voordat de kosten ontstaan.[8] Een belangenorganisatie is op grond van art. 3:305a lid 2 BW immers verplicht om eerst overleg te voeren. Samsung heeft hierdoor de mogelijkheid om de updates uit te stellen. Hoewel de beveiliging uiteindelijk wel wordt bijgewerkt, zijn de telefoons gedurende een langere periode kwetsbaar.

De Consumentenbond kan nog wel belang hebben bij een verklaring voor recht. Deze verklaring stelt de kopers van de telefoons in staat om schadevergoeding te vorderen. Een dergelijk belang ontbreekt echter als er geen aanwijzing bestaat dat de kwetsbaarheden tot schade hebben geleid. De rechtbank overweegt dat de Stagefright-kwetsbaarheden voor zover bekend nooit zijn misbruikt. Misbruik veroorzaakt bovendien niet altijd schade die voor vergoeding in aanmerking komt. De omstandigheid dat er persoonsgegevens zijn verspreid[9] of dat het apparaat deel heeft uitgemaakt van een botnet, hoeft bijvoorbeeld niet tot schade te leiden.

Een uitspraak waarin de rechter verklaart dat Samsung de Stagefright-kwetsbaarheden sneller had moeten oplossen, zou een duidelijk precedent scheppen. Zij zou suggereren dat er ook een verplichting tot het bijwerken van de software bestaat in vergelijkbare situaties. Ook dit achterliggende doel is op zichzelf echter, net als waarheidsvinding en emotionele en principiële belangen, geen belang in de zin van art. 3:303 BW.[10]

De open normen van het Nederlandse Burgerlijk Wetboek kunnen een verplichting tot het bijwerken van de beveiliging van software in het leven roepen. Het conflict tussen Samsung en de Consumentenbond laat echter zien dat het niet eenvoudig is om deze verplichting in de rechtspraak te concretiseren. Aan de ene kant is een te algemeen geformuleerde verplichting niet-toewijsbaar omdat de omstandigheden van het geval steeds anders zijn. Aan de andere kant kan het vereiste van voldoende belang een beletsel vormen bij een concretere vordering. De ontwikkeling van cybersecurityverplichtingen in de jurisprudentie blijft hierdoor achter. De uitspraak in *Consumentenbond/Samsung* suggereert dat deze situatie pas verandert als een kwetsbaarheid werkelijk tot vergoedbare schade leidt of een ontwikkelaar blijvend weigert om een reële dreiging weg te nemen. Zij functioneert hierdoor als een duidelijk argument voor de formulering van concretere juridische eisen in standaarden en regelgeving.

Mr. P.T.J. Wolters*

6. Vergelijk www.consumentenbond.nl/acties/updaten (laatst bezocht 4 juli 2018).
7. T.R. Bleeker, 'Voldoende belang in collectieve acties: drie maal artikel 3:303 BW', *NTBR* 2018, afl. 5, p. 140.
8. HR 19 maart 1993, *NJ* 1993, 304 (*Verburg/Van der Hoek Makelaardij*); HR 14 mei 1993, *NJ* 1993, 445 (*Toptas/Nederland*).
9. Zie hierover uitgebreid T.F. Walree, 'De vergoedbare schade bij de onrechtmatige verwerking van persoonsgegevens', *WPNR* 2017, afl. 7172, p. 921-930.
10. Vergelijk HR 16 april 1993, *NJ* 1993, 444 (*Alp/Nederland*); HR 14 mei 1993, *NJ* 1993, 445 (*Toptas/Nederland*); HR 9 oktober 1998, *NJ* 1998, 853 (*Jeffrey*); E. Gras, 'Over de rechtspraak inzake het emotionele belang tegen de achtergrond van art. 6 EVRM jo. 6 EUV/65 EGV', *PP* 2005, afl. 6, p. 186; Bleeker 2018, p. 140-141.

* Universitair docent burgerlijk recht en onderzoeker bij het Onderzoekcentrum Onderneming & Recht van de Radboud Universiteit.
(**P.Wolters@jur.ru.nl**)